Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures

Commissioner Robert J. Jackson Jr.

Feb. 21, 2018

I reluctantly support today's guidance in the hope that it is just the first step toward defeating those who would use technology to threaten our economy. The guidance essentially reiterates years-old staff-level views on this issue. But economists of all stripes agree that much more needs to be done. As the White House's own Council of Economic Advisers noted on Friday:

> The presence of externalities would lead firms to rationally underinvest in cybersecurity. Left to their own devices, firms will choose their optimal level of investment by conducting an analysis of private costs and benefits without taking externalities into account. In light of this market failure, regulators can devise a scheme of penalties and incentives that are designed to make firms internalize the externalities and thereby help raise levels of cybersecurity investment to the socially optimal level. For example, certain mandatory disclosure requirements were previously shown to incentivize firms to adopt better cybersecurity measures (see, e.g., Gordon et al. 2015, who conduct an analysis of externalities resulting from weak cybersecurity).
>
> * * * *
>
> [T]he effectiveness of the SEC's 2011 Guidance is frequently questioned. There are concerns that companies underreport events due to alternative interpretations of the definition of "materiality" (Gordon et al. 2006, 2015). There are also concerns that the disclosure requirements are too general and do not provide clear instructions on how much information to disclose, and that they therefore "fail to resolve the information asymmetry at which the disclosure laws are aimed" (Ferraro 2014). For example, according to the 2017 survey of 2,168 individuals who were involved in both cyber risk and enterprise risk management activities in their firms, 36 percent of survey participants said that a material loss of information assets does not require a disclosure on the firm's financial statements. At the same time, 43 percent of respondents stated that their firm would disclose a loss of property plant and equipment on its financial statements (Ponemon 2017b). According to these studies, more comprehensive and mandatory disclosure guidance, such as through legislative endorsement (Ferraro 2014) or endorsement by the SEC (Gregory 2014), may help overcome these issues.
>
> * * * *
>
> The lack of a representative data set for cybersecurity incidents poses a number of challenges to firms and policymakers. For policymakers, it makes it next to impossible to accurately measure the cost of cybersecurity incidents for the U.S. economy and to determine whether more active government involvement is needed to limit cybersecurity risk. Likewise, for firms, the lack of data makes it difficult to correctly assess the expected costs of cybersecurity exposure and to determine the optimal level of investment in cybersecurity. Moreover, when negative information is underreported for incentive reasons, agents may erroneously assume that the negative information/events simply do not exist (see, e.g., Scherbina 2008). In case of adverse cyber events, underreporting may lead the less sophisticated managers to assume that the risk is not

significant and consequently to underinvest in cybersecurity. Cybersecurity professionals speculate that less sophisticated smaller firms underinvest in cybersecurity for this reason.[1]

---

[1] White House Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy 25, 31-32, *available at* https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (February 16, 2018).